PATENT ABSTRACTS OF JAPAN

W1605

(11)Publication number : 09-212565
(43)Date of publication of application : 15.08.1997

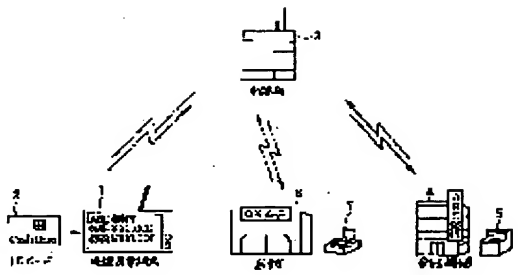
(51)Int.Cl. G06F 19/00
G06K 17/00
G07D 9/00
G07D 9/00
G07D 9/00
G07D 9/00

(21)Application number : 08-020337
(22)Date of filing : 07.02.1996

(71)Applicant : NEC CORP
(72)Inventor : WATANABE MITSUHIRO

(54) RADIO PORTABLE TERMINAL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To make a place where a user is charged unlimited and minimize the possibility that information is stolen by making a radio connection with the center terminal of a financial institution, and exchanging money information and confirming a password code.
SOLUTION: A customer inserts an IC card 2 into the radio portable terminal 1 first and inputs necessary money with input keys on the radio portable terminal 1. Then this information is inputted to the financial institution 4 through a repeater station 3 and the center terminal 5. Then necessary money is withdrawn from the account of the customer of the financial institution 4 and then the IC card 2 of the customer is charged with the money. When the customer makes a purchase at a store 6, the customer carries the IC card 2 to the store 6 and inserts it into a register terminal at the store 6, and then the money of the purchase is withdrawn from the amount of the IC card 2. The store 6 demands the financial institution 4 to pay the money through the register terminal 7, repeater station 3, and center terminal 5 according to the customer information read out of the IC card 2.



LEGAL STATUS

[Date of request for examination] 07.02.1996
[Date of sending the examiner's decision of rejection] 21.09.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

W1505

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－212565

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　19/00			Ｇ０６Ｆ　15/30	Ｃ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｌ	
Ｇ０７Ｄ　9/00	４３６		Ｇ０７Ｄ　9/00	４３６Ｚ	
	４５１			４５１Ｂ	
	４５６			４５６Ａ	

審査請求　有　請求項の数９　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平8－20337

(22)出願日　平成８年(1996)２月７日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　渡辺　光洋
東京都港区芝五丁目７番１号　日本電気株式会社内

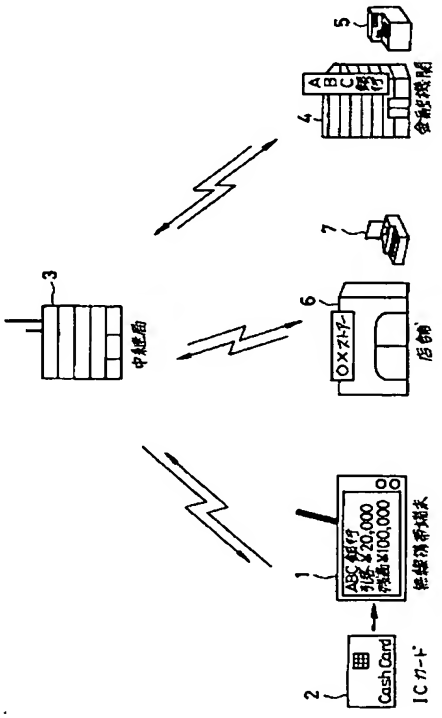
(74)代理人　弁理士　▲柳▼川　信

(54)【発明の名称】　無線携帯端末システム

(57)【要約】

【課題】　ＩＣカードに金銭をチャージする場所がＡＴＭのある場所に限定されること。

【解決手段】　中継局３を介して金融機関４の端末５と無線で接続される無線携帯端末１と、この無線携帯端末１に挿入されるＩＣカード２とで構成され、無線携帯端末１よりＩＣカード２に直接金銭情報を書き換える。また、ＩＣカード２内にチャージされる金銭残高は無線携帯端末１を介して電波により金融機関４の端末５に送信され、金融機関４はこの金銭残高を顧客の口座の残高と照合する。



【特許請求の範囲】
【請求項１】　金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含むことを特徴とする無線携帯端末システム。
【請求項２】　前記無線通信手段は前記金融機関のセンター端末と無線で接続される無線携帯端末と、この無線携帯端末に挿入されるカードとからなり、このカードは前記金融機関のセンター端末より引き落とされる金銭情報の加算および前記金融機関のセンター端末に預け入れされる金銭情報の減算が行われる演算手段と、この演算手段で演算後の残高が格納される格納手段とを有することを特徴とする請求項１記載の無線携帯端末システム。
【請求項３】　前記カードは前記暗証番号の確認を行う確認手段をさらに有することを特徴とする請求項２記載の無線携帯端末システム。
【請求項４】　前記暗証番号は前記無線携帯端末より入力され前記カードに送られることを特徴とする請求項２または３記載の無線携帯端末システム。
【請求項５】　前記暗証番号は金銭情報の保護用と金融機関アクセス情報の保護用の２種からなることを特徴とする請求項１～４いずれかに記載の無線携帯端末システム。
【請求項６】　前記無線携帯端末は第１の鍵を有し、この第１の鍵により金銭情報を暗号化して前記カード内の格納手段に格納する暗号化手段をさらに有することを特徴とする請求項２～５いずれかに記載の無線携帯端末システム。
【請求項７】　前記無線携帯端末は第２の鍵を有し、この第２の鍵により前記暗号化された金銭情報を復号化して読み出す復号化手段をさらに有することを特徴とする請求項６記載の無線携帯端末システム。
【請求項８】　前記カードは前記無線携帯端末より第２の鍵を受取り、前記暗号化された金銭情報を復号化して読み出す第２の復号化手段をさらに有することを特徴とする請求項６記載の無線携帯端末システム。
【請求項９】　前記無線携帯端末は、前記カードに電源を供給する電源供給手段を有することを特徴とする請求項２～８いずれかに記載の無線携帯端末システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は無線携帯端末システムに関し、とくにＩＣカードにより金融機関と金銭の授受を行う無線携帯端末システムに関する。
【０００２】
【従来の技術】ＩＣカードにより金融機関と金銭の授受を行う、いわゆる電子財布システムは知られている。
【０００３】この電子財布システムは、銀行、各種金融機関が顧客に予めＩＣカードを発行しておき、顧客が買物をする際、ＡＴＭ（現金自動支払機）より、現金の代わりに金銭データをＩＣカードに書き込み、顧客は店で買物した金額をこのＩＣカードにより支払うシステムである。
【０００４】この電子財布システムは、顧客が現金を持ち歩く必要がない点、および店から銀行に売上金を運搬する現金輸送車が不要である点等から安全性が高く、効率的である。
【０００５】また、たとえばプリペイドカード（料金先払いカード）の場合であれば、予め表示された金額を使い果たすとそのカードでさらに買物をすることはできなかったが、電子財布システムではＩＣカードに記憶された金額がゼロとなっても、そのＩＣカードに設けられたテンキーにより新たに必要な金額を追加することで、さらに買物をすることができる。もっとも、その追加する金額が自己の口座に存在することが前提となるのはいうまでもない。
【０００６】このような電子財布システムの一例が特開平３－９２９６６号公報および特開平５－９４４５８号公報に開示されている。
【０００７】特開平３－９２９６６号公報に開示された技術は、ＩＣカードに表示部と入力キーとを持たせ、小型のコンピュータの機能を持たせながら、ＩＣカードを使用する際はこのＩＣカードに電源を入れ、パスワードを入力してから現金の引き落とし、またはプリペイドカード機能を使用するものであり、特開平５－９４４５８号公報に開示された技術は、ＩＣカードおよび店舗取引端末で構成される電子財布システムにおいて、その認証手段に必要な銀行鍵を個人ごとにユニークにし、さらにこれを時間可変な鍵とするものである。
【０００８】
【発明が解決しようとする課題】しかし、従来の電子財布システムは、まず第１にＩＣカードに金銭をチャージする（金額を書き込む）場所および時間が限定されるという欠点がある。
【０００９】これは、金銭をチャージする場所は各金融機関に設置されているＡＴＭ（Ａｕｔｏｍａｔｉｃ　Ｔｅｌｌｅｒ　Ｍａｃｈｉｎｅ；現金自動預金払出機）に限定されるということである。
【００１０】第２にＩＣカードを紛失したり盗難されたりすると、第三者にＩＣカードの情報を盗まれる可能性が大きくなるという欠点がある。
【００１１】これは、従来のＩＣカードは暗証番号および金額を入力するための入力キーおよび金額の表示部を備えているため、このキー入力により暗証番号が一致すれば金銭の使用が可能となるためである。
【００１２】第３にＩＣカードの使用方法が複雑であるという欠点がある。
【００１３】これは、銀行などのＡＴＭから金銭をチャージする場合は、このＩＣカードの入力キーで暗証番号を打ち込み、ＩＣカードを起動させてからＡＴＭのカー

ド差し込みロに挿入し、さらにＡＴＭの暗証番号を打ち込むという二重の操作を行わなければならないということである。また、このＩＣカードをプリペイトカード代わりに店舗で使用する場合も、まずカードの電源を入れ、次にＩＣカードに暗証番号を打ち込んでＩＣカードを稼働状態にしてから使用するという手順を踏まなければならないことである。

【００１４】第４にＩＣカードが電池切れになるとＩＣカードの使用ができなくなるという欠点がある。

【００１５】これは、ＩＣカードを起動ためには電池が必要だからである。当然ながら電池がなくなりＩＣカードを起動することができなければ、金銭をＩＣカードにチャージできないばかりか、ＩＣカードにチャージされた金銭を使用することさえできなくなる。

【００１６】そこで本発明の目的は、金銭をチャージする場所が限定されず、ＩＣカードを紛失等しても第三者にＩＣカードの情報を盗まれる可能性が少なく、ＩＣカードの使用方法が容易で、かつＩＣカードの電池切れという事態を回避することができる無線携帯端末システムを提供することにある。

【００１７】

【課題を解決するための手段】前記課題を解決するために本発明は、金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含むことを特徴とする。

【００１８】

【発明の実施の形態】本発明によれば、金融機関のセンター端末と顧客の携帯端末とを無線で接続し、金融機関の自己の口座より金銭を携帯端末にチャージする。

【００１９】以下、本発明の実施例について添付図面を参照しながら説明する。図１は本発明に係る無線携帯端末システムの構成図である。

【００２０】無線携帯端末システムは、無線携帯端末１と、この無線携帯端末１に挿入されるＩＣカード２とからなり、この無線携帯端末１の通信は中継局３を経由して金融機関４のセンター端末５および店舗６のレジ端末７と無線で行われる。

【００２１】金融機関４には各顧客の金銭情報が管理されている。顧客はまず無線携帯端末１にＩＣカード２を挿入し、無線携帯端末１上の入力キーより必要な金銭を打ち込む。するとこの情報は中継局３およびセンター端末５を経由して金融機関４に入力される。そして、その必要な金銭が金融機関４のその顧客の口座から差し引きされ、次いで顧客のＩＣカード２にその金銭がチャージされる。

【００２２】顧客が店舗６で買物する場合は、そのＩＣカード２をその店舗２に持参し、そのＩＣカード２を店舗６内のレジ端末７に挿入すると、買物した金銭がそのＩＣカードから差し引かれる。店舗６はそのＩＣカード２から読み出した顧客情報をもとにレジ端末７、中継局３およびセンター端末５を経由して金融機関４に対し金銭の支払いを請求する。これに対し、金融機関４は先にＩＣカード用として差し引かれた顧客の金銭から必要な金銭を店舗６の口座に振り込む。

【００２３】次に、無線携帯端末１の構成について説明する。図２は無線携帯端末の一実施例の構成図である。

【００２４】無線携帯端末１は、ＣＰＵ（中央処理演算ユニット）１１と、クロックジェネレータ１２と、バスコントローラ１３と、ＤＭＡ（Ｄｉｎａｍｉｃ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）コントローラ１４と、マスクＲＯＭ１５と、フラッシュメモリ１６と、ＤＲＡＭ（ダイナミックＲＡＭ）１７と、ＬＣＤ（液晶表示器）１８と、タッチパネル１９と、ＰＷＭ（音声）出力２０と、無線部２１と、メモリインタフェース２２と、ＬＣＤインタフェース２３と、Ｉ／Ｏインタフェース２４と、無線部インタフェース２５と、ＩＣカード用電源２６とからなる。

【００２５】ＣＰＵ１１は、本発明である無線携帯端末１のソフトウエアを実行するための心臓部であり、本無線携帯端末１のＯＳおよびアプリケーションプログラムを実行する部分である。ＯＳ部はマルチタスク方式になっており、各電子決済プログラム等のアプリケーションソフトの実行と無線のプロトコル、タッチパネル１９の補正等の処理を時分割で実行する。

【００２６】クロックジェネレータ１２はクロック発生部である。

【００２７】バスコントローラ１３は、ＣＰＵ１１とメモリインタフェース２２、ＣＰＵ１１とＬＣＤインタフェース２３、ＣＰＵ１１とＩ／Ｏインタフェース２４、ＣＰＵ１１と無線部インタフェース２５、ＤＭＡ１４による転送を主体としたメモリインタフェース２２とＬＣＤインタフェース２３、メモリインタフェース２２とＩ／Ｏインタフェース２４、メモリインタフェース２２と無線部インタフェース２５夫々の間のデータ転送についてアービトレーション（調停）を行う。

【００２８】ＤＭＡ１４は各メモリ１５～１７とＬＣＤ１８、各インタフェース２２～２５、無線間のデータをＣＰＵ１１がメインバスにアクセスしていない空き時間にデータを自動で転送する。

【００２９】マスクＲＯＭ１５は、無線携帯端末のＯＳや基本アプリケーションを格納するためのＲＯＭである。

【００３０】フラッシュメモリ１６には、本システムのＯＳ、無線のプロトコルを実行するためのドライバ、財布の機能を実現するための金銭管理プログラム、金銭情報・店名番号・口座番号・暗証番号等の暗号化・復号化プログラム、ＩＣカード２のリード・ライト用のプロトコルを実行するためのドライバ、タッチパネル１９のドライバ、音声コーデックのドライバが基本プログラムと

して内蔵される。

【００３１】ＤＲＡＭ１７は、主にアプリケーションのワーク、ＬＣＤ１８のＶＲＡＭ（ビデオＲＡＭ）、Ｉ／Ｏに接続される周辺ブロックのワーク、無線部インタフェース２５の受信データの保存用として使用される。

【００３２】ＬＣＤ１８は、本無線携帯端末システムの表示媒体であり、金融機関４へアクセスを行う際のガイド情報、金銭情報を引き出す際に使用する暗礁番号の書き換え画面等を表示する。

【００３３】タッチパネル１９は、本無線携帯端末システムの入力手段であり、ＬＣＤ表示画面の上に載せて使用し、ＬＣＤ１８の表示位置とタッチパネル１９の入力位置をリンクさせてＬＣＤ１８上に表示された疑似的なタイプライタやテンキー、ボタン等を押すとその応答をＬＣＤ１８に表示させ、押されたことを確認できるような形にする。

【００３４】ＰＷＭ出力２０は、音声を出力する部分であり、前述した金融機関４へアクセスを行う際に画面情報と併せて音声ガイドを行う。

【００３５】無線部２１は、本システムの通信手段である。無線、たとえばＰａｇｅｒ（ポケットベル）等の電波は構造上ビルの中でも突き抜けて使用できるため、無線を使用することでどこの場所にいても金銭を引き出すことができる。

【００３６】メモリインタフェース２２は、マスクＲＯＭや、追加アプリケーションやＩＣカード２のバックアップ情報を格納するためのフラッシュメモリ１６とワークエリアや無線携帯端末の受信データを格納するためのＤＲＡＭ１７にアクセスするためのインタフェース機能を持つ。

【００３７】ＬＣＤインタフェース２３は、ＬＣＤ１８とＣＰＵ１１，ＤＭＡ１４間の信号のやりとりを中継する。ＤＲＡＭ１７上のバッファに蓄えられたＬＣＤ１８の表示データはＤＭＡ１４を使用してＬＣＤ１８に転送されるが、ＬＣＤインタフェース２３はＤＲＡＭ１７に書き込まれた階層情報を含んだＬＣＤデータをＬＣＤ１８の表示データに変換する機能を併せ持つ。

【００３８】Ｉ／Ｏインタフェース２４には、金銭情報を書き込むためのＩＣカード２、手書きデータを入力したりデータの選択を行ったりするための入力手段であるタッチパネル１９、ユーザインタフェースとして応答に使用する音声出力２０が接続される。

【００３９】無線部インタフェース２５は、中継局３と無線携帯端末１間のデータをやりとりするための通信回路である無線部２１とのインタフェースおよび無線部レジスタとのインタフェースを受け持つ。

【００４０】ＩＣカード用電源２６はＩＣカード２に電源を供給するためのものである。

【００４１】なお、このＩ／Ｏインタフェース２４と接続されるＩＣカード２は、後述するが内部にメモリを備えたクレジットカードサイズのメモリであるが、本システムではこのＩＣカード２にＣＰＵも搭載することでＩＣカード２をインテリジェント化させ、任意の入力データに対し演算処理を施して外部に結果を返せるようにする。

【００４２】次に各インタフェースの構成について説明する。図３はバスコントローラ１３の構成図である。バスコントローラ１３は、ＤＲＡＭリフレッシュジェネレータ３１と、アービター（調停部）３２と、アドレスデコーダ３３とからなる。

【００４３】ＤＲＡＭリフレッシュジェネレータ３１は、ＤＲＡＭ１７に対してメモリのリフレッシュを行うための信号を作り出すためのタイミングをカウントし、アービター３２に対しリフレッシュの要求を行う部分である。

【００４４】アービター３２は、ＣＰＵ１１とメモリ間等、各インタフェース２２～２５のデータバスがぶつからないようにアービトレーション（調停）を行う部分である。夫々のインタフェース２２～２５には優先順位を付けて夫々のインタフェースからバスのアクセス要求が来たときに優先順位の高いものから順番にバスを開放する役目を担う。

【００４５】アドレスデコーダ３３は、前もって決めておいた各インタフェース２２～２５のアドレス領域をＣＰＵ１１がアクセスしたときの選択信号を生成する部分である。

【００４６】なお、同図に示す入出力信号は信号名および行き先のみを示し、動作説明は省略する。以下、図７まで同様である。

【００４７】図４はメモリインタフェース２２の構成図である。メモリインタフェース２２は、ＤＲＡＭアドレスジェネレータ４１と、フラッシュアドレスジェネレータ４２と、Ｄバスサイジング４３と、ＲＤＹシグナルジェネレータ４４と、リフレッシュシグナルジェネレータ４５と、ＲＡＳ・ＣＡＳジェネレータ４６とからなる。

【００４８】ＤＲＡＭアドレスジェネレータ４１は、ＣＰＵ１１がＤＲＡＭ１７にアクセスを行うときのＣＰＵ１１のアドレスをＤＲＡＭ１７用のＲＡＳ・ＣＡＳアドレスに変換する部分である。

【００４９】フラッシュアドレスジェネレータ４２は、ＣＰＵ１１がフラッシュメモリ１６にアクセスを行うときのＣＰＵ１１のアドレスをフラッシュメモリ１６のアドレスに変換する部分である。フラッシュメモリ１６のアクセス方式は、ＤＲＡＭ１７のようにＲＡＳ・ＣＡＳでアクセスする方式や、フルアドレスでアクセスする方式があるので使用するメモリの種類によって対応させる必要がある。

【００５０】Ｄバスサイジング４３は、ＣＰＵ１１のデータバスのビット幅を各メモリ用のビット幅に変換する部分である。

【００５１】たとえば、ＣＰＵ１１のビット幅が１６ビットで、メモリのビット幅が８ビットのとき、ＣＰＵ１１の１６ビット幅のデータを上位８ビットと下位８ビットの２回に分けてメモリに書き込むようにする。

【００５２】ＲＤＹシグナルジェネレータ４４は、バスコントローラ１３からのＩＦ・ＡＤＳ信号に対してのＲＤＹ（ＲＥＡＤＹ）信号を生成する部分である。

【００５３】リフレッシュシグナルジェネレータ４５は、バスコントローラ１３のリフレッシュ信号をトリガとして、夫々のＤＲＡＭ１７ごとのリフレッシュタイミングに合わせてＲＡＳ・ＣＡＳを合成する部分である。

【００５４】ＲＡＳ・ＣＡＳジェネレータ４６は、ＤＲＡＭ１７に対してのアクセス信号、およびリフレッシュ信号を生成する部分である。

【００５５】図５はＬＣＤインタフェース２３の構成図である。ＬＣＤインタフェース２３は、コントロールシグナルジェネレータ５１と、バスサイジング５２と、フィールド５３と、セレクタ５４とからなる。

【００５６】コントロールシグナルジェネレータ５１は、表示媒体であるＬＣＤ１８のコントロール信号を生成する部分であり、ＬＣＤ１８のフレーム番号、ラインデータロード信号、ＬＣＤ駆動電圧交流化信号、シフトレジスタのクロックパルス信号等が含まれる。

【００５７】図６はＩ／Ｏインタフェース２４の構成図である。Ｉ／Ｏインタフェース２４は、アドレスデコーダ６１と、コントロールシグナルジェネレータ６２と、セレクタ６３，６４とからなる。

【００５８】アドレスデコーダ６１は、Ｉ／Ｏへのアクセスがカード２であるか、音声出力２０であるか、タッチパネル１９であるかをセレクトする信号とＩ／Ｏ部のレジスタをセレクトする信号を生成する部分である。

【００５９】コントロールシグナルジェネレータ６２は、ＩＣカード２、音声出力２０、タッチパネル１９に対する制御信号を生成する部分で、たとえばＩＣカード２に対してはクロックやリセット信号等を生成する。

【００６０】セレクタ６３，６４は、各データの入出力の方向を選択するものである。

【００６１】図７は無線部インタフェース２５の構成図である。無線部インタフェース２５は、アドレスデコーダ７１と、バスサイジング７２と、コントロールシグナルジェネレータ７３とからなる。

【００６２】アドレスデコーダ７１は、無線部２１のレジスタをセレクトするための信号を生成する。

【００６３】バスサイジング７２は、ＣＰＵ１１のデータバスのビット幅を無線データのビット幅に変換する部分である。

【００６４】コントロールシグナルジェネレータ７３は、無線部２１のコントロール信号を生成する部分である。

【００６５】次に、ＩＣカード２の構成について説明する。図８はＩＣカード２の構成図である。

【００６６】ＩＣカード２は、ＣＰＵ８１と、メモリインタフェース８２と、メモリＭｅｍ１，Ｍｅｍ２と、シリアルインタフェース８３と、シリアルＩ／Ｏ８４とからなる。

【００６７】ＣＰＵ８１は、ＩＣカード２の演算処理部で暗証番号の確認、その他金銭の加算・減算等の処理を行う。

【００６８】メモリＭｅｍ１，Ｍｅｍ２はＣＰＵ１１の実行するプログラムの格納や実行時のワークエリアとして使用する。

【００６９】メモリインタフェース８２はこれらのメモリとＣＰＵ１１間のインタフェースフェースを取り持つ。

【００７０】このようにメモリ領域をＭｅｍ１とＭｅｍ２とに分けたのは、セキュリティを強化するためである。すなわち、外部にシリアルＩ／Ｏ８５を介して出力するデータはＭｅｍ２の領域のみを見せて、Ｍｅｍ１の領域はＩＣカード２の暗証番号を入れない限り、無意味なデータしか読めず、書き込みは不可能とする機能をこのＩＣカード２に持たせる。

【００７１】シリアルＩ／Ｏ８４は、ＩＣカード２のデータの入出力部である。ＩＣカード２はこの部分を通してＩＤ情報や金銭情報等の各種データを出し入れする。

【００７２】シリアルインタフェース８３は、このＩ／Ｏ８４とＣＰＵ８１間のインタフェースを取り持つ。

【００７３】次に、ＩＣカード２の動作について説明する。まず第１に、ＩＣカード２に保存する情報であるが、ＩＣカード２にはカードが本人のものであることを確認するためのＩＤ情報と金融機関にアクセスするための暗証番号を書き込む。この情報はＩＣカード２のＭｅｍ１に格納しておく。

【００７４】ＩＤ情報の中身はＩＣカードが提携している金融機関の銀行番号、店番号、科目、口座番号、顧客の名前等であり、暗証番号の中身は無線携帯端末１を使用して金融機関との現金授受プログラムを起動させるための暗証番号Ａと、各金融機関ごとの暗証番号Ｂの２種類を持たせる。

【００７５】ここで、暗証番号Ａは顧客が無線携帯端末１を扱いＩＣカード２のＩＤ情報を確認したり、金融機関にアクセスするための前処理のための暗証番号であるため、この暗証番号は顧客が後から書き換えられるものとする。

【００７６】一方、暗証番号Ｂは各金融機関ごとに固有のものであるため、顧客が提携している銀行が複数あれば、複数の暗証番号が必要となる。また、この暗証番号Ｂは金融機関と契約された暗証番号であるため、顧客側では勝手に書き換えることはできない。

【００７７】また、本システムに使用するＩＣカード２

は、いわゆるプリペイドカードと同様な機能も持たせる必要があるため、ＩＣカード２内に蓄えられている金銭情報は第三者にも確認できる必要がある。その反面、個人情報、ＩＤ情報、暗証番号等、他人には知られたくないデータも同時にこのＩＣカード２に書き込む必要がある。

【００７８】そこで、前述したＭｅｍ２に金銭情報を格納し、Ｍｅｍ１に個人情報、ＩＤ情報、暗証番号等を格納する。これにより、第三者は金銭情報は読み出せるが、個人情報、ＩＤ情報、暗証番号等は読み出せないことになる。

【００７９】図９はＩＣカードの読み書き制御を示すフローチャートである。外部からシリアルＩ／Ｏ８４を介して入力されたコマンドをＣＰＵ８１が解析し、そのコマンドに対する応答結果を再びシリアルＩ／Ｏ８４を介して外部に返すという形式をとる。

【００８０】まず、外部よりメモリリードのコマンドがＩＣカード２に入力されると（Ｓ１）、ＣＰＵ８１はＭｅｍ１のマスクが解除されているかを調べる（Ｓ２）。

【００８１】後述するが、暗証番号Ａが確認されていないとこのマスクは解除されない。したがって、第三者が入力したコマンドであればＭｅｍ１のマスクは解除されていないので、ＣＰＵ８１は外部にダミーデータ（でたらめなデータ）を出力する（Ｓ３）。一方、顧客が入力したコマンドであればＭｅｍ１のマスクは解除されているので、正規データが出力される（Ｓ４）。

【００８２】同様に、外部よりメモリライトのコマンドがＩＣカード２に入力されると（Ｓ５）、ＣＰＵ８１はＭｅｍ１のマスクが解除されているかを調べる（Ｓ６）。第三者が入力したコマンドであればＭｅｍ１のマスクは解除されていないので、ＣＰＵ８１はライトコマンドを無視する（Ｓ７）。一方、顧客が入力したメモリライトのコマンドであればＭｅｍ１のマスクは解除されているので、正規データが出力される（Ｓ８）。

【００８３】外部より暗証番号Ａ相当のデータがＩＣカード２に入力されると、ＣＰＵ８１は暗証番号Ａかどうかを確認する（Ｓ１０）、そして暗証番号Ａと確認するとマスクを解除する（Ｓ１１）。一方、暗証番号Ａと確認しなければエラーコードを出力する（Ｓ１２）。

【００８４】外部より暗証番号Ｂ相当のデータがＩＣカード２に入力されると、ＣＰＵ８１は暗証番号Ｂかどうかを確認する（Ｓ１５）、そして暗証番号Ｂと確認するとマスクが解除されているかを確認する（Ｓ１６）。もし、顧客であれば、後述するがまず暗証番号Ａを入力しているはずであり、この場合はマスクは解除されている。したがって、マスクは解除されているので金融機関へのアクセスが可能となる（Ｓ１７）。一方、暗証番号Ｂと仮に（偶然に）確認された場合であっても、これが第三者によるものであれば、暗証番号Ａは確認されていないはずであるから、マスクは解除されていない。したがって、この場合はエラーコードを出力する（Ｓ１８）。また、Ｓ１５に戻り、Ｓ１５で暗証番号Ｂが確認されない場合はエラーコードを出力する（Ｓ１８）。

【００８５】図１０は金銭授受プログラムを起動させる手順を示すフローチャートである。図１０において暗証番号Ａを入力する手順は本無線携帯端末１に接続されるＩＣカード２のＩＤ情報を読み書きできるモードに移行させるための手段である。このモードはＩＣカード２の所有者がＩＤ情報を確認する場合にも適用される。これを行うことで第三者にカードの中身を知られないようにする。

【００８６】暗証番号Ｂを入力する手順は金融機関４に預けている預金を引き出したり預けたりする場合に使用する。

【００８７】この場合も暗証番号の処理はＩＣカード２内部で行うようにし、電波に乗せて外部に情報が漏れることのないようにする。

【００８８】暗証番号Ａは顧客が所定のプログラムで自由に書き換えられるようにし、暗証番号ＢはＩＣカード２を発行する際に金融機関４側で書き込み、顧客は自由に書き換えはできないようにする。

【００８９】この場合の所定のプログラムとは無線携帯端末１側に入っている。但し、ＩＣカード２内に記載されている暗証番号Ａの書き換えは、前回設定された番号をＩＣカード２が確認したときのみ行えるようにし、この書き換えを実際に行うのはＩＣカード２であることはいうまでもない。

【００９０】次に、フローの詳細について説明する。同図の左側が無線携帯端末１のフロー、右側がＩＣカード２のフローである。

【００９１】まず、無線携帯端末１へＩＣカード２を挿入し、無線携帯端末１のタッチパネルより暗証番号Ａを入力すると、無線携帯端末１よりＩＣカード２へリクエスト信号が送出される（Ｓ２１）。これに対し、ＩＣカード２より確認（Ａｃｋ）信号が返送される（Ｓ２２）。この確認信号を受けると、無線携帯端末１よりＩＣカード２へ暗証番号Ａが送信され、暗証番号Ａ確認のプログラムが起動する（Ｓ２３）。

【００９２】すると、ＩＣカード２は暗証番号Ａの確認を行い、本人のものと確認されない場合は異常終了を示すエラーコードを無線携帯端末１へ返送し（Ｓ２４）、動作を終了させる（Ｓ２５）。

【００９３】一方、暗証番号Ａが本人のものと確認された場合は正常確認コードを無線携帯端末１へ返送し（Ｓ２６）、正常終了させる（Ｓ２７）。これにより、ＩＣカード２のシークレットエリアは解除される（Ｓ２８）。すなわち、Ｍｅｍ１の内容の読み出し、書き込みが可能となる。これで、金融機関４との通信が確立する（Ｓ２９）。

【００９４】金融機関４との通信が確立すると、無線携

帯端末１のタッチパネルより暗証番号Ｂを入力する。すると、無線携帯端末１よりＩＣカード２へリクエスト信号が送出される（Ｓ３０）。このリクエスト信号を受けると、ＩＣカード２は暗証番号Ｂ確認のプログラムを起動し（Ｓ２３）、無線携帯端末１へ確認信号を返送する（Ｓ３２）。

【００９５】この確認信号が無線携帯端末１で受信されると、無線携帯端末１より暗証番号ＢがＩＣカード２に送信される（Ｓ３３）。次に、ＩＣカード２では暗証番号Ｂの確認が行われ（Ｓ３４）、金融機関４が本人のものと確認されると正常確認コードが無線携帯端末１に返送される（Ｓ３５）。

【００９６】一方、本人のものと確認されない場合は、異常終了を示すエラーコードが無線携帯端末１に返送される（Ｓ３６）。なお、異常終了の場合は３回まで暗証番号Ｂの再入力が認められるが（Ｓ３７）、３回入力しても異常終了となる場合はＩＣカード２は動作を異常終了させる（Ｓ３８）。そして、この場合、無線携帯端末１より金融機関４に対し、このＩＣカード２の不正使用の情報が送信される（Ｓ３９）。

【００９７】正常確認コードが無線携帯端末１に返送されると、無線携帯端末１よりＩＣカード２に対する金銭の入出力が可能となる（Ｓ４０）。すると、無線携帯端末１よりＩＣカード２に対しカード残高書き換え要求信号が送信され、これに対する確認信号が無線携帯端末１に返送されると（Ｓ４２）、ＩＣカード２では残高の書き換えが行われる（Ｓ４３）。

【００９８】残高の書き換えが終了すると、無線携帯端末１よりＩＣカード２に対しシークレットエリア起動要求信号が送信され（Ｓ４４）、これを受信したＩＣカード２は確認信号を返送する（Ｓ４５）。そして、ＩＣカード２のＭｅｍ１は再び読み出し書き込みができなくなる。

【００９９】次に、ＩＣカード２の金銭情報の変更が無線携帯端末１より金融機関４へ送信され、動作は終了する。

【０１００】尚、ＩＤ情報等のＩＣカード２のデータを無線携帯端末１側に読み込むためには秘密鍵を使用する必要がある。秘密鍵は後で述べる暗証番号Ｂを利用する。

【０１０１】まず、ＩＣカード２のシークレットエリアを開放するための暗証番号ＡをＩＣカード２に転送してＩＣカード２のシークレットエリアであるＩＤ領域を開放する。これによりＩＣカード２による預金引き出し可能状態となる。

【０１０２】次に金融機関４にアクセスするための暗証番号Ｂを入力する。無線携帯端末１は暗証番号ＢをＩＣカード２に転送し、ＩＣカード２は暗証番号Ｂを受け取ったら、これを秘密鍵として公開鍵と併せて内部データの暗証番号Ｂの復号化を行う。

【０１０３】次に復号化された暗証番号Ｂと入力された暗証番号Ｂが一致するかどうか確認し、一致したら図１０の引き出しまたは預金金額の入力プロセスに移行する。

【０１０４】預金取引終了後、ＩＣカード２内の暗証番号Ｂによる復号化の際のバッファは全て消去する。また、無線携帯端末１側はＩＣカード２の切断が確認され次第、内部バッファにためられている暗証番号Ｂに関するバッファを全て消去する。これはＩＣカード２アクセス中に無理矢理、無線携帯端末１とＩＣカード２との接続を切られた場合にも適用する。

【０１０５】このＩＣカード２をプリペイドカードとして使用するときは、先に述べたとおり第三者がＩＣカード２の金銭情報を読み書きできなければならない。

【０１０６】このとき、第三者またはこのカード２の持ち主が金銭情報を勝手に書き換えて金額を増やすといったことはできないようにする必要がある。

【０１０７】その方法を図１１に示す。図１１は金銭情報書き換えのプロテクトの手順を示すフローチャートである。

【０１０８】金銭の加算（Ｓ５１）については無線携帯端末１が金融機関４との接続を行っていることを確認し（Ｓ５２）、接続できているときは、加算金額分だけＩＣカード２に加算するようにし（Ｓ５３）、接続ができていないときは、ＩＣカード２はエラーコードを返してコマンド待ちに戻るようにしておく（Ｓ５４）。この接続の確認は、暗証番号Ａ，暗証番号Ｂの入力が確認され、更に金融機関４からの接続ＯＫのコードを無線携帯端末１から受け取ったときにＩＣカード２は接続ＯＫフラグを立てる。このフラグが立っているときは前回の金銭に加算金額分だけ値を増やす。

【０１０９】金銭の減算（Ｓ５６）についてはこの確認は行わず、減算金額分だけ前回の金額から値を減らす（Ｓ５７）。

【０１１０】また、ＩＣカード２内のデータは全て暗号化しておく。暗号化にはＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）やＦＥＡＬ（高速データ暗号化処理手順）などの共通鍵の方式を取ることもできるし、更に安全性を確保するにはＲＳＡ（暗号化方式の一種）などの公開鍵の方式を取ることも考えられる。

【０１１１】暗号化を行うにはまず暗号化の鍵となる物が必要になる。また暗号化されたデータを復号化するための鍵がなければデータを復号できない。

【０１１２】共通鍵の方式とはこの暗号化と復号化の鍵を同一にする方式である。一方、公開鍵の方式とは暗号化を行うには鍵Ａのみで行えるが復号化を行うには鍵Ａと鍵Ｂを必要とする方式である。鍵Ａは鍵Ｂから生成される鍵で鍵Ａからは鍵Ｂは合成できない。この鍵Ａを公開鍵と予備鍵Ｂを秘密鍵と呼んでいる。

【０１１３】例として図１２に公開鍵の方式でＩＣカー

ド２のデータに暗号化をかけた例を示す。図１２は暗号化及び復号化の手順のフローチャートである。まず、同図（Ａ）の暗号化について説明する。

【０１１４】携帯無線端末１上に蓄えられているデータまたはＩＣカード２から読み取ったデータを平文とし暗号をかけるための鍵を公開鍵、公開鍵によって暗号化されたデータを暗号文とする。ＩＣカード２のデータは他人に容易には読めないように暗号化をして保存をしておく必要がある。

【０１１５】この暗号化をＩＣカード２より処理能力の大きい無線携帯端末１側で行う。まず暗号化されていない平文を先に述べた公開鍵により、暗号化する（Ｓ８１）。暗号化の終了した暗号文は随時ＩＣカード２側に送信する（Ｓ８２）。この様にすることで、たとえカード２を何らかの手段で手に入れた自分以外の者が中身のデータを読み込めたとしても暗号化されたデータが入っているだけで、他の者には復号化しない限り意味のあるデータにならないため悪用されることはない。

【０１１６】一方、復号時のパターンとしてはＡ，Ｂの２種類が考えられる。まず復号時同図（Ｂ）について説明を行う。同図（Ｂ）はＩＣカード２内に公開鍵を予め書き込んでおいて復号化をＩＣカード２内で行う方式である。復号時は顧客が無線携帯端末１の入力手段から秘密鍵を打ち込み（Ｓ６１）、その鍵をＩＣカード２に転送し（Ｓ６２）、ＩＣカード２は無線携帯端末１から受け取った秘密鍵と予め書き込まれている公開鍵を利用してＩＣカード２内に書き込まれている暗号文を復号化し（Ｓ６３）、無線携帯端末１に復号化された後の平文を転送する（Ｓ６４）。

【０１１７】この様にすると復号化の処理がＩＣカード２内で完結するため、他の端末から暗号化されたデータを読み出す事もＢの方式に比べ容易にできる。

【０１１８】次に復号時同図（Ｃ）について説明を行う。同図（Ｃ）はＩＣカード２内の暗号化されたデータをＩＣカード２に比べ処理能力の高い無線携帯端末１側で復号化することができる。

【０１１９】暗号化されたデータを復号化するには、まず無線携帯端末１はＩＣカード２に内部の暗号文を転送してもらう（Ｓ７１）。データの読み込みが終了したら、入力手段により無線携帯端末１に秘密鍵を打ち込む（Ｓ７２）。無線携帯端末１は、この秘密鍵と予め書き込まれている公開鍵を使用して、先にＩＣカード２から読み取った暗号文を復号化する。

【０１２０】この方法の時に他の端末でＩＣカード２の内容を読む場合には、赤外線等の無線またはＲＳ－２３２Ｃなどの有線によって他の端末に公開鍵を転送した後復号化を行うということが考えられる。

【０１２１】次に図１２で使用する公開鍵の作成の手段及びその使用方法例，また秘密鍵の作成手段及びその使用方法例を示す。

【０１２２】公開鍵は金融機関４毎の暗証番号Ｂ（これを秘密鍵にする）とＩＣカード２のシリアルナンバーから生成する。金融機関４は、まず最初にＩＣカード２へＩＤ情報，暗証番号Ｂの登録を行う必要があるのとＩＣカード２を発行する側なのでシリアルナンバーは当然知っている。ゆえに公開鍵の生成は金融機関４側で行う。金融機関４は公開鍵生成後、公開鍵により暗号化されたＩＤ情報と平文の公開鍵をＩＣカード２に書き込みを行い、その後ＩＣカード２を顧客に送る。

【０１２３】このときＩＤ情報は図８のＭｅｍ１に書き込む必要があり、ここにアクセスするために暗証番号Ａを必要とする。暗証番号Ａは顧客が自由に書き換え可能な番号であるが、ＩＣカード２を発行する際のデフォルト（省略）では暗証番号を入力しないでおく。そうすれば、顧客は最初にＩＣカード２のＩＤ情報を見る時には暗証番号を入力することなしにＩＤ情報にアクセスすることができる。

【０１２４】顧客はＩＣカード２を受け取ったら、まず最初に無線携帯端末１とＩＣカード２を接続し無線携帯端末１に公開鍵の設定を行う。無線携帯端末１側はＩＣカード２が接続されたのを確認した後、公開鍵のデータ引き渡し要求をＩＣカード２に送る。ＩＣカード２は要求を受け取ったら、無線携帯端末１側に公開鍵を転送する。無線携帯端末１側は公開鍵を受け取ったら内部のメモリに公開鍵の情報をバックアップする。これで無線携帯端末１側の初期設定は終了である。無線携帯端末１側は次回よりＩＣカード２にデータを書き込む際はこの公開鍵を基に暗号化を行った上で行う。

【０１２５】ＩＣカード２を使用して店舗６などで品物を購入する際は、店舗６側が予め金融機関４とＩＣカード２の使用契約をしておく。この際にＩＣカード２のＩＤ情報を読み出すための種別コードを金融機関４からもらう。この種別コードを店舗６側が持っているＩＣカード２専用のレジ端末７に登録しておく。

【０１２６】レジ端末７はＩＣカード２が接続されたら自分の種別コードをＩＣカード２に転送する。ＩＣカード２はレジ端末７の種別コードを受け取ったら、ＩＤ領域を開放し金銭情報を引き出せる状態に移行する。

【０１２７】チャージされている金銭を取り出すときはＩＣカード２に金銭の取り出し要求を発行し、ＩＣカード２は要求された金額分だけチャージされた金銭を減らし内部メモリＭｅｍ２の金銭情報を書き換える。書き換えが正常に終了したらＡＣＫを返す。要求金額が残金より大きいなどで書き替えが正常に行えない場合は、異常終了コード及びエラーコードを返し内部メモリの金銭情報の書き換えは行わない。

【０１２８】レジ端末７側は前もってＩＣカード２にチャージされている残金が分かっているので、取り出す金額がＩＣカード２の残金よりも大きい場合は残金分だけの要求をＩＣカード２に行う。

【０１２９】また、銀行などで現金を引き出す場合はＡＴＭ側が出力する自分の種別コードをＩＣカード２側に送ることで、ＩＣカード２は内部のシークレット領域をＩＤ情報の領域のみ開放しＡＴＭからＩＤ情報を読み出せるようにする。また、ＡＴＭにより現金を引き出すときは図１０で示した暗証番号Ｂを利用して金銭をＩＣカード２にチャージするのと同様な方法で現金を引き出せるようにする。

【０１３０】但し、ＩＣカード２への金銭チャージは暗証番号Ａを入力して、ＩＣカード２の全領域を開放しないとできないようにしておく。

【０１３１】また本発明に使用する無線通信は双方向に通信できる手段であればＰａｇｅｒ（ポケットベル）以外のＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙｐｈｏｎｅ　Ｓｙｓｔｅｍ）やセルラーなどの方式でも構わないし、ＩＣカード２についても内部にＣＰＵを内蔵できる機構であればＰＣＭＣＳＡ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ　Ｍｅｍｏｒｙ　Ｃａｒｄ　Ｓｔａｎｄａｒｄ　Ａｓｓｏｃｉａｔｉｏｎ）などのカードでも問題ない。

【０１３２】また、無線携帯端末１内にＩＣカード２に電源を供給するための電源２６を備えたので、ＩＣカード２用の電池は不要となる。

【０１３３】

【発明の効果】本発明によれば、第１に金融機関のセンター端末と無線で接続され、金銭情報のやりとりと暗証番号の確認を行うことで金銭情報の引き落としおよび預け入れを行う無線通信手段を含み携帯端末システムを構成したので、金銭情報の引き落としおよび預け入れをＡＴＭのない場所でも行うことができる。また、時間が限定されるということもない。

【０１３４】第２にＩＣカードに入力キー、表示部を備えないため、第三者に暗証番号を不正に入力されるおそれがない。また、仮になんらかの方法で暗証番号が入力され、内部の金銭情報が読み出されたとしても金銭情報は予め暗号化されているため、容易に読み出すことは困難である。

【０１３５】第３に、暗証番号の入力は無線携帯端末に対して行うだけで済むので使用方法が簡易となる。また、ＩＣカードを店舗で使用する場合でも店舗のレジ端末に対する操作のみで済むため使用方法が簡易となる。

【０１３６】第４に、ＩＣカードの電源供給は無線携帯端末より行うため、ＩＣカードの電池が不要となる。したがって、電池切れで使用不可能という事態を回避することができる。また、ＩＣカード２のみでは作動しないため不正使用の防止にもなる。

【図面の簡単な説明】

【図１】本発明に係る無線携帯端末システムの構成図である。

【図２】同システムの無線携帯端末の一実施例の構成図である。

【図３】同システムのバスコントローラの構成図である。

【図４】同システムのメモリインタフェースの構成図である。

【図５】同システムのＬＣＤインタフェースの構成図である。

【図６】同システムのＩ／Ｏインタフェースの構成図である。

【図７】同システムの無線部インタフェースの構成図である。

【図８】同システムのＩＣカードの構成図である。

【図９】同システムのＩＣカードの読み書き制御を示すフローチャートである。

【図１０】同システムの金銭授受プログラムを起動させる手順を示すフローチャートである。

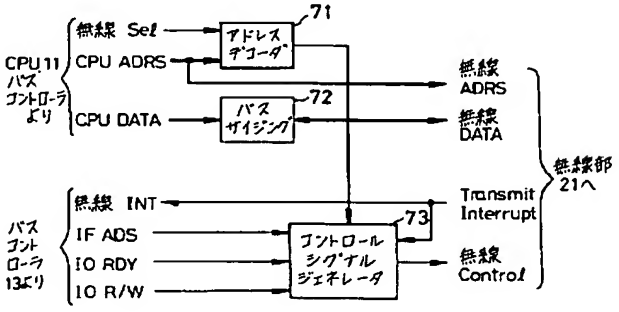
【図１１】同システムの金銭情報書き換えプロテクトの手順を示すフローチャートである。

【図１２】同システムの暗号化および復号化の手順を示すフローチャートである。

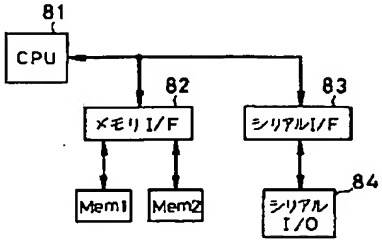
【符号の説明】

１　無線携帯端末
２　ＩＣカード
４　金融機関
５　センター端末
２６　電源

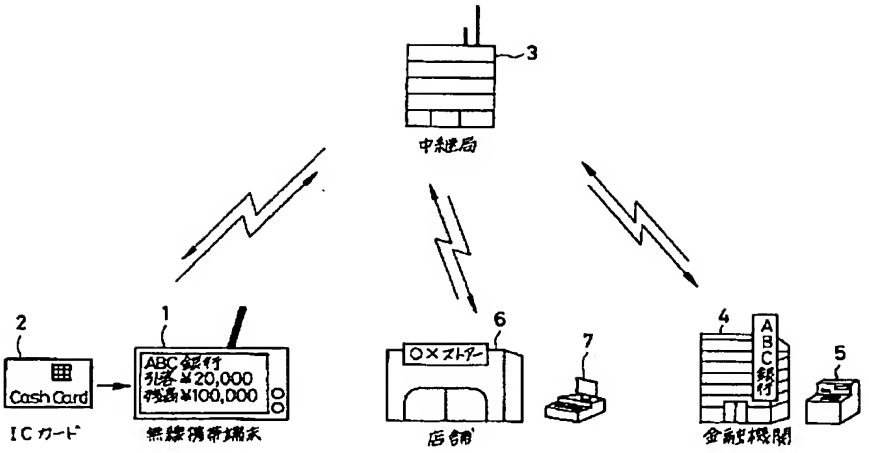
【図７】



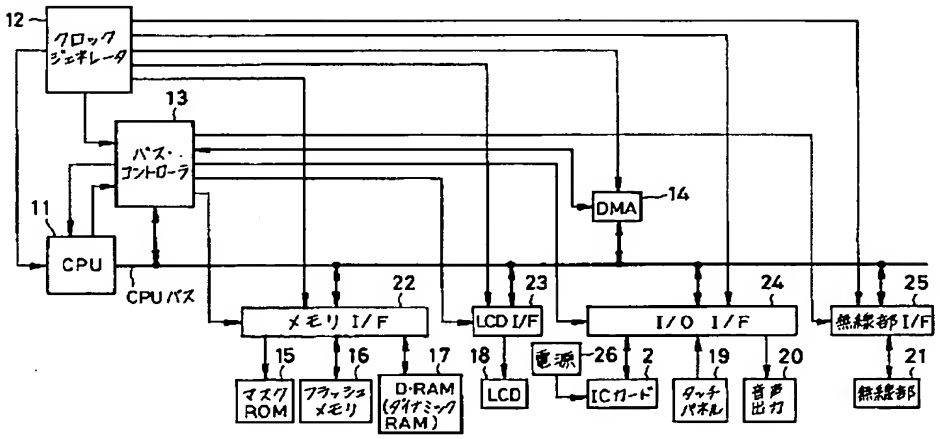
【図８】



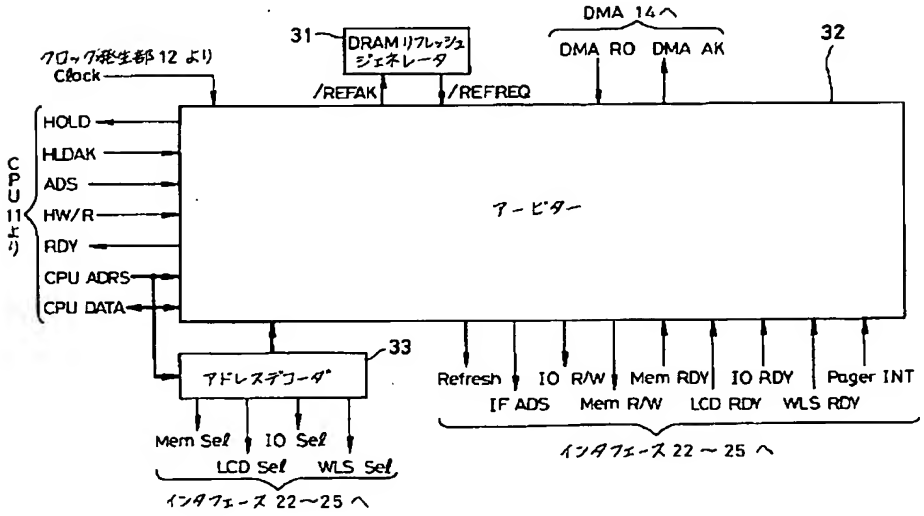
【図１】


3
中継局
2
Cash Card
ICカード
1
ABC銀行
引落 ¥20,000
残高 ¥100,000
無線携帯端末
6
○×ストア
店舗
7
4
ABC銀行
5
金融機関

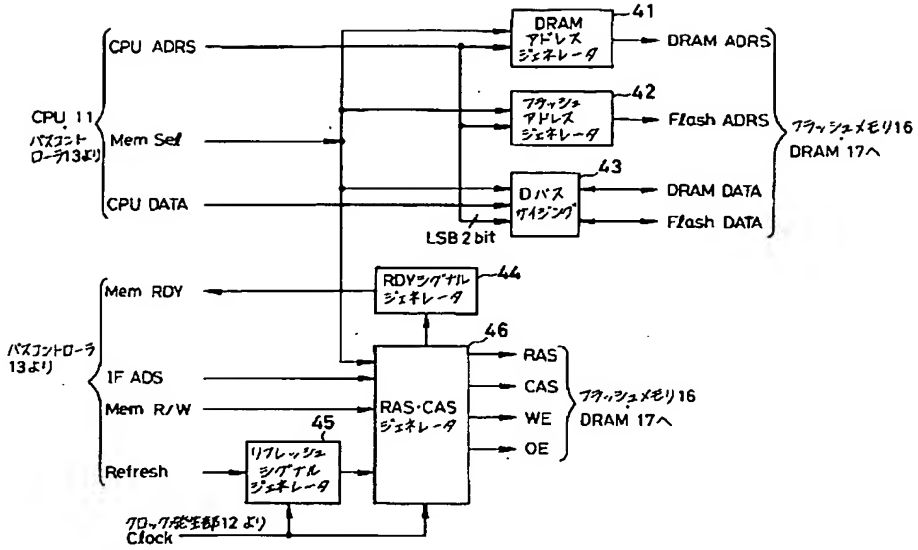
【図２】


12
クロック ジェネレータ
13
バス・コントローラ
11
CPU
CPUバス
DMA
14
22
メモリ I/F
23
LCD I/F
24
I/O I/F
25
無線部 I/F
15
マスクROM
16
フラッシュメモリ
17
D-RAM (ダイナミックRAM)
18
LCD
電源
26
2
ICカード
19
タッチパネル
20
音声出力
21
無線部

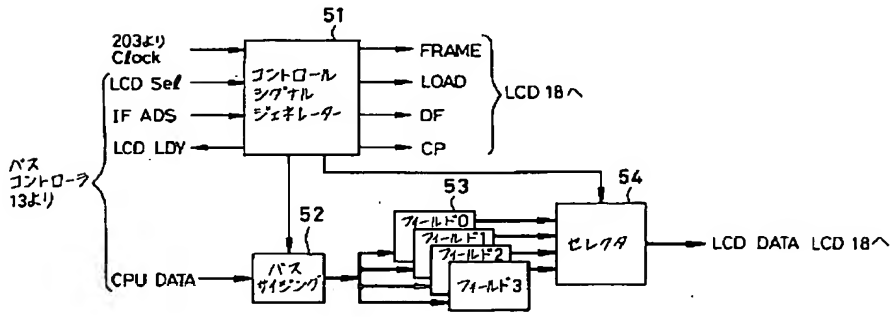
【図３】


クロック発生部12より
Clock
31
DRAMリフレッシュジェネレータ
/REFAK
/REFREQ
DMA 14へ
DMA RQ
DMA AK
32
CPU 11より
HOLD
HLDAK
ADS
HW/R
RDY
CPU ADRS
CPU DATA
アービター
33
アドレスデコーダ
Mem Sel
IO Sel
LCD Sel
WLS Sel
インタフェース 22～25へ
Refresh
IO R/W
Mem RDY
IO RDY
Pager INT
IF ADS
Mem R/W
LCD RDY
WLS RDY
インタフェース 22～25へ

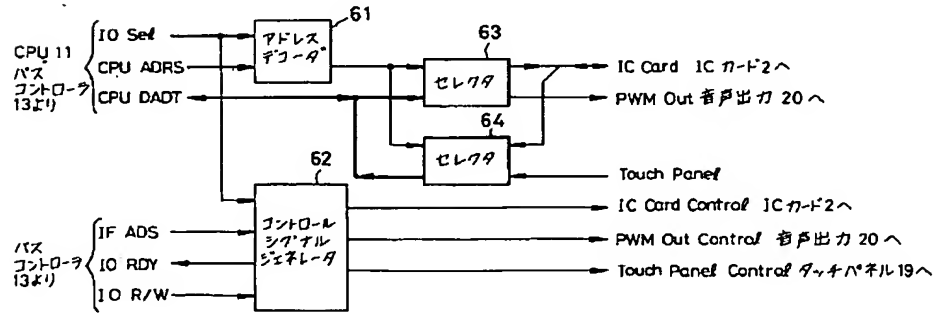
【図4】


CPU ADRS
CPU 11
バスコントローラ13より
Mem Sel
CPU DATA
DRAM アドレス ジェネレータ
41
DRAM ADRS
フラッシュ アドレス ジェネレータ
42
Flash ADRS
フラッシュメモリ16 DRAM 17へ
Dバス サイジング
43
DRAM DATA
Flash DATA
LSB 2 bit
Mem RDY
RDYシグナル ジェネレータ
44
バスコントローラ 13より
IF ADS
Mem R/W
Refresh
46
RAS
CAS
WE
OE
フラッシュメモリ16 DRAM 17へ
RAS・CAS ジェネレータ
45
リフレッシュ シグナル ジェネレータ
クロック発生部12より
Clock

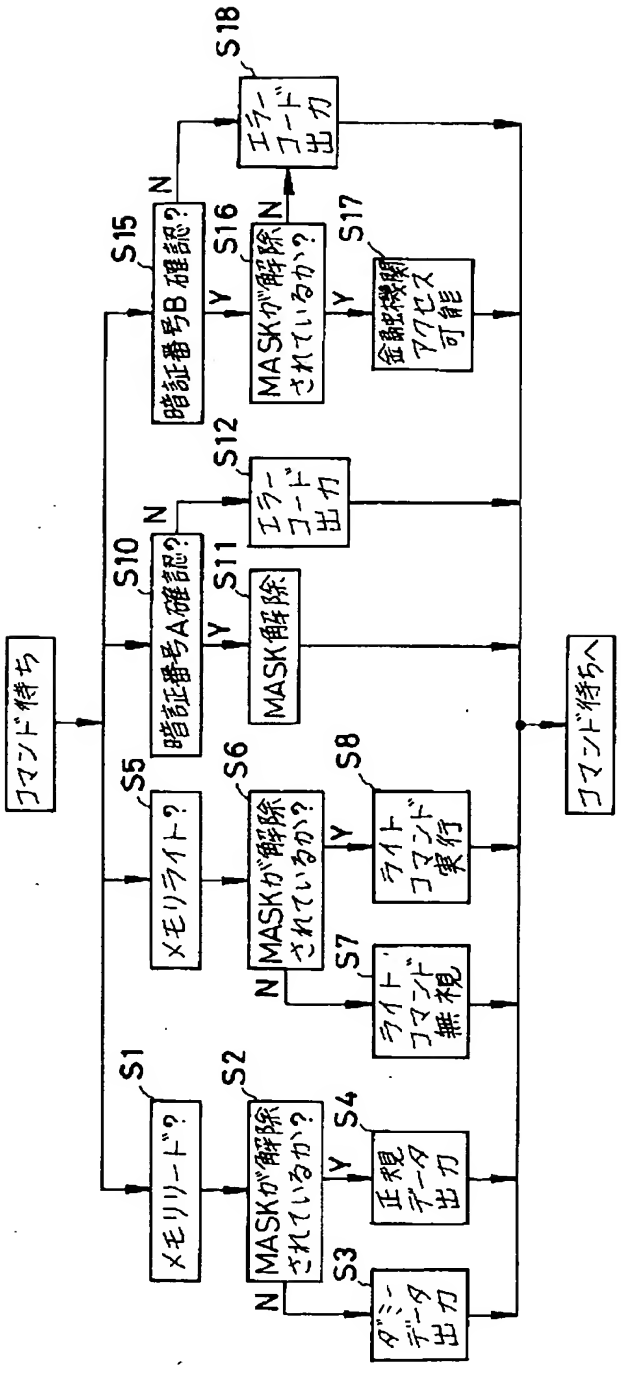
【図5】


51
203より Clock
LCD Sel
IF ADS
LCD LDY
コントロール シグナル ジェネレーター
FRAME
LOAD
DF
CP
LCD 18へ
バス コントローラ 13より
54
53
52
フィールド0
フィールド1
フィールド2
フィールド3
セレクタ
LCD DATA LCD 18へ
CPU DATA
バス サイジング

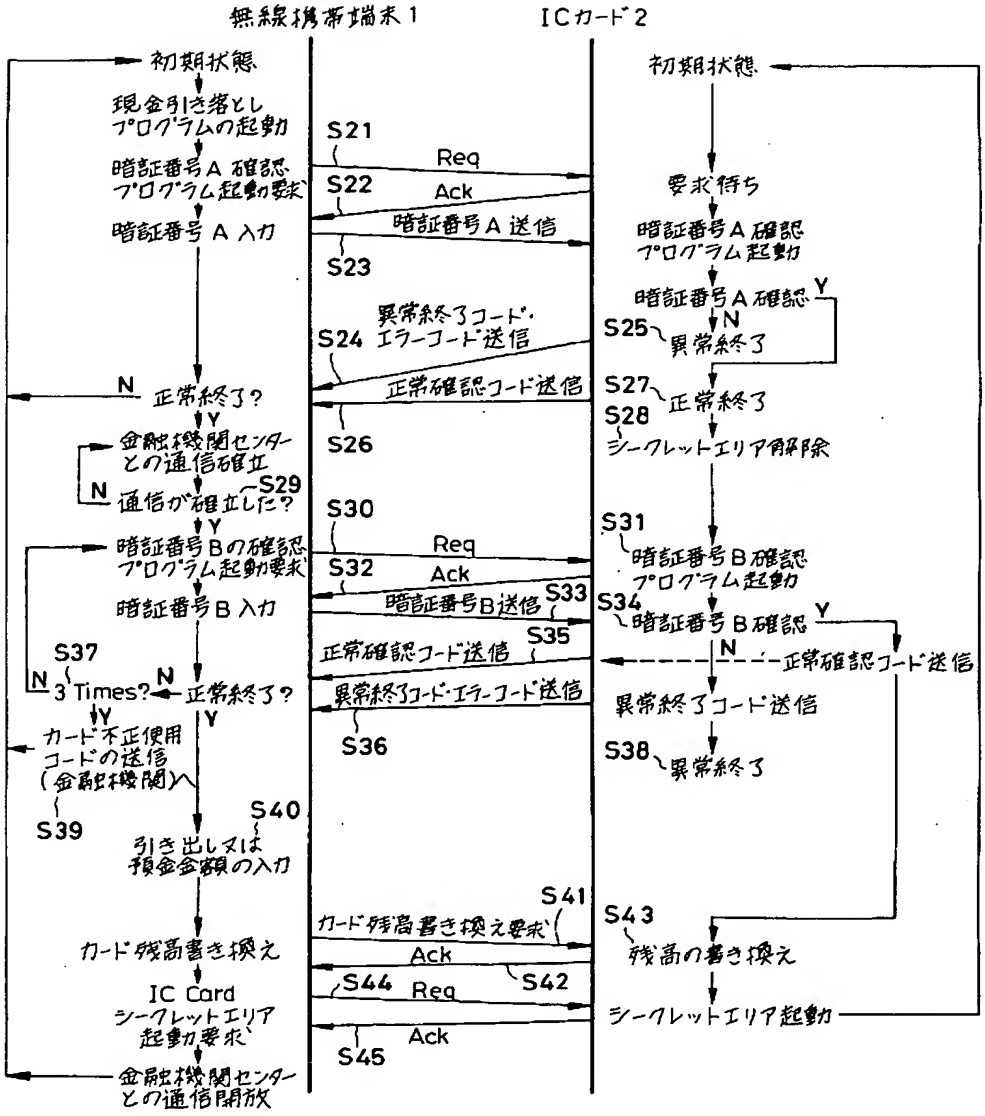
【図6】


CPU 11
バス コントローラ 13より
IO Sel
CPU ADRS
CPU DADT
アドレス デコーダ
61
63
セレクタ
IC Card IC カード2へ
PWM Out 音声出力 20へ
64
セレクタ
Touch Panel
62
IC Card Control IC カード2へ
PWM Out Control 音声出力 20へ
Touch Panel Control タッチパネル19へ
バス コントローラ 13より
IF ADS
IO RDY
IO R/W
コントロール シグナル ジェネレータ

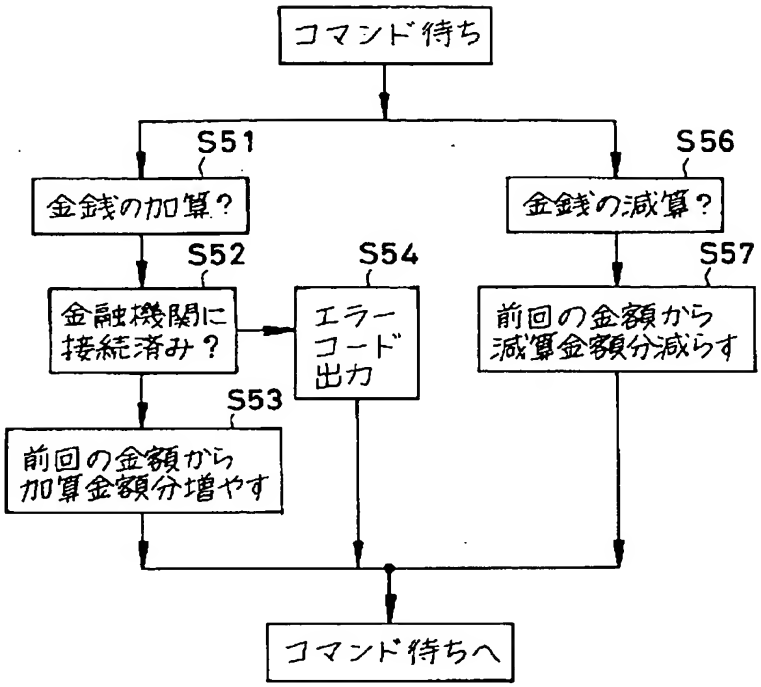
【図９】


コマンド待ち
S1
メモリリード?
S2
MASKが解除されているか?
S3
ダミーデータ出力
S4
正規データ出力
S5
メモリライト?
S6
MASKが解除されているか?
S7
ライトコマンド無視
S8
ライトコマンド実行
S10
暗証番号A確認?
S11
MASK解除
S12
エラーコード出力
S15
暗証番号B確認?
S16
MASKが解除されているか?
S17
金融機関アクセス可能
S18
エラーコード出力
コマンド待ちへ
Y
N

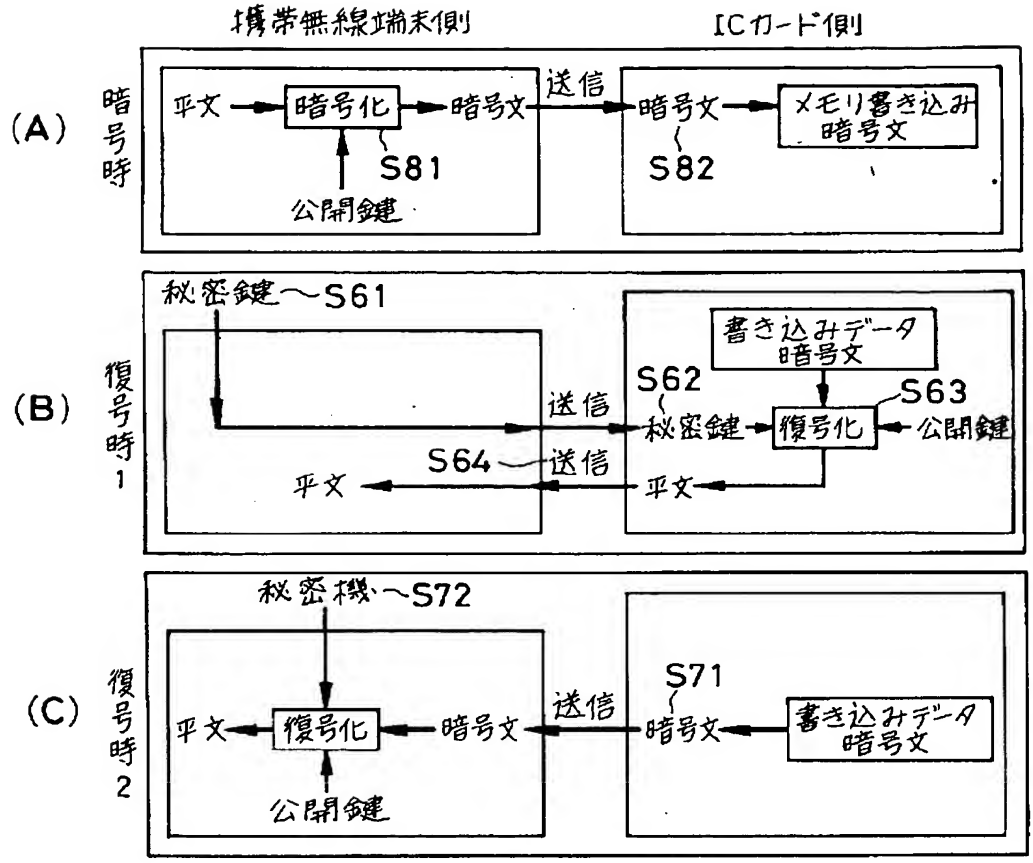
【図１０】


無線携帯端末１
ICカード２
初期状態
現金引き落とし
プログラムの起動
暗証番号Ａ確認
プログラム起動要求
暗証番号Ａ入力
S21
Req
S22
Ack
暗証番号Ａ送信
S23
異常終了コード・
エラーコード送信
S24
正常確認コード送信
S26
N
正常終了？
Y
金融機関センター
との通信確立
N
通信が確立した？
S29
Y
暗証番号Ｂの確認
プログラム起動要求
S30
Req
S32
Ack
暗証番号Ｂ送信
S33
暗証番号Ｂ入力
S37
N
3 Times?
N
正常終了？
Y
Y
カード不正使用
コードの送信
（金融機関）
S39
S40
引き出しヌは
預金金額の入力
カード残高書き換え
IC Card
シークレットエリア
起動要求
金融機関センター
との通信開放
初期状態
要求待ち
暗証番号Ａ確認
プログラム起動
暗証番号Ａ確認
Y
N
S25
異常終了
S27
正常終了
S28
シークレットエリア解除
S31
暗証番号Ｂ確認
プログラム起動
S34
暗証番号Ｂ確認
Y
N
正常確認コード送信
異常終了コード送信
S38
異常終了
S35
正常確認コード送信
異常終了コード・エラーコード送信
S36
S41
カード残高書き換え要求
Ack
S42
S44
Req
Ack
S45
S43
残高の書き換え
シークレットエリア起動

【図１１】


コマンド待ち
S51
金銭の加算？
S56
金銭の減算？
S52
金融機関に接続済み？
S54
エラーコード出力
S57
前回の金額から減算金額分減らす
S53
前回の金額から加算金額分増やす
コマンド待ちへ

【図１２】



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	FI		技術表示箇所
G07D 9/00	461		G07D 9/00	461B	
			G06F 15/30	350	
				360	